NO. 17-15611-BB

IN THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff/appellee,

 \mathbf{v} .

SCOTT JOSEPH TRADER,

Defendant/appellant.

On Appeal from the United States District Court For the Southern District of Florida

> BRIEF OF THE APPELLANT SCOTT JOSEPH TRADER

> > MICHAEL CARUSO Federal Public Defender

Fletcher Peacock
Assistant Federal Public Defender
Attorney for Appellant Trader
109 North 2nd Street
Fort Pierce, Florida 34950
Tel. (772) 489-2123

THIS CASE IS ENTITLED TO PREFERENCE (CRIMINAL APPEAL)

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Scott Joseph Trader Case No. 17-15611-BB

Appellant files this Certificate of Interested Persons and Corporate Disclosure Statement, listing the parties and entities interested in this appeal, as required by 11th Cir. R. 26.1.

Barnes, Antonia J., Assistant United States Attorney Cannon, Aileen M., Assistant United States Attorney Caruso, Michael, Federal Public Defender Ferrer, Wifredo A., Former United States Attorney Greenberg, Benjamin G., Acting United States Attorney Gyires, Marton, Assistant United States Attorney Hopkins, Hon, James M., United States Magistrate Judge Marks, Neison, Assistant Federal Public Defender Matthewman, Hon. William, United States Magistrate Judge Maynard, Hon. Shaniek M., United States Magistrate Judge Middlebrooks, Hon. Donald M., United States District Judge Militello, Kristy, Assistant Federal Public Defender Peacock, R. Fletcher, Assistant Federal Public Defender

Smachetti, Emily M., Assistant United States Attorney

Trader, Scott Joseph, Defendant/Appellant

United States of America, Plaintiff/Appellee

Villafana, Marie, Assistant United States Attorney

<u>s/Fletcher Peacock</u> Fletcher Peacock, AFPD

STATEMENT REGARDING ORAL ARGUMENT

Appellant respectfully submits that oral argument is necessary to the just resolution of this appeal and will significantly enhance the decision-making process.

TABLE OF CONTENTS

Certificate of Interested Persons
Statement Regarding Oral Argumenti
Table of Citationsiv
Statement of Subject Matter and Appellate Jurisdiction
Statement of the Issues2
Statement of the Case
Course of Proceedings and Disposition in the District Court3
Statement of Facts4
Standard of Review11
Summary of the Argument
Arguments and Citations of Authority14
1. Whether the government's procurement of the
defendant's "Kik" subscriber records, including location
information, without a warrant was a violation of Mr.
Trader's reasonable privacy expectation under the
Fourth Amendment14

2.	Whether the affidavit in support of the warrant to	
	search Mr. Trader's home failed to show probable cause	
	on its face	22
3.	Whether Mr. Trader's sentence of life imprisonment	
	was substantively unreasonable.	27
Conclusio	n	39
Certificat	e of Compliance	40
Certificat	e of Service	41

TABLE OF CITATIONS

CASES:

Andresen v. Maryland,
427 U.S. 463, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976)24
Carpenter v. United States,
U.S, 138 S.Ct. 2206 (2018)12, 15-17, 21
Dorman v. United States,
140 U.S.App.D.C. 313 (1970)
Gall v. United States,
552 U.S. 38, 128 S.Ct. 586 (2007)
Government Accountability Project v. U.S. Department of State,
699 F.Supp. 2d 97 (D.C. 2010)20
Katz v. United States,
389 U.S. 347, 88 S.Ct. 507 (1967)
Kennedy v. Louisiana,
554 U.S. 407, 128 S. Ct. 2641 (2008)
Kimbrough v. United States,
552 U.S. 85, 128 S. Ct. 558 (2007)

Kyllo v. United States,
533 U.S. 27, 121 S.Ct. 2038 (2001)14
Payton v. New York,
445 U.S. 573, 100 S.Ct. 1371 (198018
Smith v. Maryland,
442 U.S. 735, 99 S.Ct. 2577 (1979)
United States v. Beiermann,
599 F. Supp. 2d 1087 (N.D. Iowa 2009)32
United States v. Booker,
543 U.S. 220, 125 S. Ct. 738 (2005)
United States v. Campa,
459 F.3d 117438
United States v. Carpenter,
819 F. 3d 880 (6th Cir. 2017)
United States v. Carter,
110 F.3d 759 (11th Cir. 1997)21
United States v. Contreras-Rodriguez,
291 Fed. Appx. 989 (11th Cir. 2008)24

United States v. Davis,
785 F.3d 498 (11th Cir. 2015)16-17, 21
United States v. Diaz,
720 F. Supp. 2d 1039 (E.D. Wis. 2010)
United States v. Dorvee,
616 F.3d 174 (2nd Cir. 2010)32
United States v. Grober,
624 F.3d 592 (3rd Cir. 2010)32
United States v. Hansen,
956 F.2d 245 (11th Cir. 1992)21
United States v. Hastie,
854 F.3d 1298 (11th Cir. 2017)20
United States v. Irey,
612 F.3d 1160 (11th Cir. 2010)
United States v. Leon,
468 U.S. 897, 104 S.Ct. 3405 (1984)24-26
United States v. Martin,
297 F.3d 1308 (11th Cir. 2002)23

United States v. Miller,	
24 F.3d 1357 (11th Cir. 1994)	11
United States v. Miller,	
425 U.S. 435, 96 S.Ct. 1619 (1976)	15
United States v. Robinson,	
62 F.3d 1325 (11th Cir. 1995)	11
United States v. Stone,	
575 F.3d 83 (1st Cir. 2009)	32
United States v. Taxacher,	
902 F.2d 867 (11th Cir. 1990)	26
United States v. Watkins,	
760 F.3d 1271 (11th Cir. 2014)	11
STATUTORY AND OTHER AUTHORITY:	
U.S. Const. amend. IV	passim
5 Ill. Comp. Stat. 140/7(1)(c)	20
18 U.S.C. § 2251(a)	3
18 U.S.C. § 2251(e)	3
18 U.S.C. § 2252(a)(2)	3
18 U.S.C. § 2252(a)(4)(B)	3

18 U.S.C. § 2252(b)(1)
18 U.S.C. § 2252(b)(2)
18 U.S.C. § 2422(b)
18 U.S.C. § 2702(b)14
18 U.S.C. § 2702(c)
18 U.S.C. § 2721
18 U.S.C. § 32311
18 U.S.C. § 3553(a)
18 U.S.C. § 3553(a)(2)(A)
18 U.S.C. § 3553(a)(2)(B)
18 U.S.C. § 3553(a)(5)
18 U.S.C. § 3553(a)(6)
18 U.S.C. § 37421
28 U.S.C. § 1291
80 Fed. Reg. 36594 (June 25, 2015)
Cal. Gov't Code § 6254.420
O.C.G.A. § 50–18–72(20)(A)
Γex. Gov't Code § 552.102(a)20
U.S.S.G. § 2A1.1

U.S.S.G. § 2A3.1
U.S.S.G. § 2G2.1
U.S.S.G. § 2G2.231-32, 35
U.S.S.G. § 4A1.2
U.S.S.G. § 4A4.1
U.S.S.G. § 4A5.1
U.S.S.G. § 4B1.5(b)
U.S. Sentencing Commission, Report to Congress:
Federal Child Pornography Offenses xii-xiii (2012)31-33
U.S. Sentencing Guidelines Manual,
Ch. 1, Pt. A, intra. comment (2015)30
Five Reasons You Shouldn't Give Out Your Email Address,
Adam Levin, ABC News, http://abcnews.go.com/Business
/reasons-give-email-candy/story?id=3137396619
What Is An IP Address And What Can It Reveal About You,
Cale Weissman, Business Insider, 2015, http://
www.businessinsider.com/ip-address-what-they-can-reveal
<u>-about-you-2015-5</u> 19

STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

The district court had jurisdiction of this case pursuant to 18 U.S.C. § 3231 because the defendant was charged with an offense against the laws of the United States. The Court of Appeals has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291 and 18 U.S.C. § 3742, which give the courts of appeals jurisdiction over all final decisions and sentences of the district courts of the United States. The appeal was timely filed on December 18, 2017, from the final judgment and commitment order (DE 40) entered on December 8, 2017, that disposes of all claims between the parties to this cause.

STATEMENT OF THE ISSUES

ISSUE I

Whether the government's procurement of the defendant's "Kik" subscriber records, including location information, without a warrant was a violation of Mr. Trader's reasonable privacy expectation under the Fourth Amendment.

ISSUE II

Whether the affidavit in support of the warrant to search Mr.

Trader's home failed to show probable cause on its face.

ISSUE III

Whether Mr. Trader's sentence of life imprisonment was substantively unreasonable.

STATEMENT OF THE CASE

The appellant was the defendant in the district court and will be referred to by name. The appellee, United States of America, will be referred to as the government. The record will be noted by reference to the document number, and page number of the Record on Appeal.

Mr. Trader is currently incarcerated.

Course of Proceedings and Disposition in the District Court

On June 13, 2017, Mr. Trader was charged by indictment with: Count 1, enticing a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b); Count 2, distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); Count 3, possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); and Counts 4 and 5, enticement of a minor to produce a sexually explicit video, in violation of 18 U.S.C. § 2251(a) and (e). (DE 7).

On September 6, 2017, Mr. Trader filed a motion to suppress illegally obtained evidence. (DE 13). The government responded. (DE 14). On September 25, 2017, the district court denied the motion and entered a written order. (DE 15).

Mr. Trader entered a conditional plea of guilty to Counts 1 – 5 on September 29, 2017, expressly reserving his right to appeal. (DE 18). The United States Probation Office concluded that Mr. Trader's Sentencing Guideline range was life imprisonment, based upon an offense level of 43 and a criminal history category of III. Presentence Investigation Report (PSR). Mr. Trader filed a motion requesting a downward variance. (DE 34).

On December 7, 2017, the district court sentenced Mr. Trader to life imprisonment and a life time term of supervised release. (DE 37). Mr. Trader filed a timely notice of appeal on December 18, 2017. (DE 44).

Statement of Facts

On May 30, 2017, the police department of Thomasville, North Carolina received a complaint that several unknown men had engaged in inappropriate on-line sexual chats with the complainant's nine year old step-daughter, had sent the girl images of child pornography, and had requested that the girl send nude images of herself. (DE 1). The Thomasville police then contacted the U.S. Department of Homeland Security (HSI).

An HSI special agent in North Carolina inspected the girl's computer tablet and learned that the girl was accessing the social media service "Say Hi." "Say Hi" is a social media application for adults 18 and older. On her profile page, the girl claimed to be "Vitoria Jones," an adult, and had posted two "self-images" which appeared to be a woman in her late twenties. (DE 1).

The review further revealed that the suspect user went by the name "Scott." (DE 1).

"Vitoria" began the "Say Hi" chat session with "Scott" by contacting him and asking: "Hi boyfriend. Can you chat please." "Vitoria" then told "Scott" that she had a gift, "Jojo bows," for his kids. "Vitoria" then requested that "Scott" send pictures of his kids. "Scott" sent two pictures of fully clothed children and asks "Vitoria" to send a photo of her child. "Vitoria" sent a picture of a clothed adolescent female and made the comment: "My kids are cute," followed by "I know honey our kids are cute." To this point, "Vitoria" was clearly posing as an adult female with minor female children. Presentence Report (PSR), at 5.

¹ Apparently, "Jojo Bows" are large colorful hair bows popular among adolescent females.

"Scott" then asked "Vitoria" to send a picture of "your daughter naked." "Vitoria" responded: "Yours frist." (sic). "Scott" responded by sending what appears to be a widely circulated Internet nude image of an apparent adolescent female along with the statement: "My youngest daughter." Approximately one minute later "Scott" sent a second nude female apparent adolescent image, also widely circulated on the Internet, and the comment: "My oldest daughter." "Vitoria" then sent two nude images of an adolescent female to "Scott." "Scott" then sent a short video of what appears to be an adult male rubbing his penis on the vagina of an adolescent female. He chatted that the video was "Me and my daughter." (PSR at 5–8).

Approximately 20 minutes later, "Vitoria" again contacted "Scott" on "Say Hi" and sent "Scott" two nude images of herself. "Vitoria" requested nude photos of "Scott." "Scott" sent a short video of a man masturbating and two still photos of an erect penis. "Vitoria" then requested a photo of "Scott's" face. "Scott" sent a still photo of an adult male's face. The image allegedly matched the facial image posted on "Scott's" "Say Hi" user profile page. All communications between the girl and Scott took place over the "Say Hi" application. (PSR at 5–8).

HSI Special Agent Cory Brant who was investigating the complaint, noticed that "Scott's" user profile on "Say Hi" indicated that he also was active on another social media service, "KiK," under the user name "Daddyhasafunnyface." Because "Say Hi" is a China-based company, Agent Brant was concerned that any request to "Say Hi" for "Scott's" subscriber records would take too long. Consequently, he sent an "Emergency Situation Disclosure Request by Law Enforcement" to "KiK" instead. In that emergency request, Agent Brant claimed that the request involved a situation "involving death or serious physical injury." Agent Brant then stated: "The KiK user identified below is believed to be actively molesting and sexually exploiting a minor in his custody and/or control. This subject is also involved in the sexual Agent Brant requested that "KiK" exploitation of other minors." produce "the last known customer name and email address and recent IP addresses used by the account holder." Agent Brant failed to inform "KiK" that its service was not used in the suspected illegal activity. (DE 1).

"KiK" responded with 29 pages, listing the "basic subscriber information, and the most recent 30 days of IP addresses if available

associated with the Kik user name you provided." The "subscriber information" included the email address associated with the "KiK" account, "strader0227@yahoo.com." It also showed that there were 594 logins to the "Daddyhasafunnyface" account from 42 different IP addresses during the 30 days prior to May 31, 2017. (DE 1).

Armed with the IP addresses and the email address, Agent Brant then sent an additional emergency disclosure demand to Comcast Corporation, the Internet provider for IP address "76.110.46.46.234 on 05/31/2017 at 6:36:32 UTC." In that request, Agent Brant described the "This subject is believed to have raped his emergency as follows: daughter last night and sent videos depicting the rape to others. Since it appears that this subject is raping a child under his custody or control and the offenses are actively taking place this emergency request is being sought." In the next section of the request, Agent Brant states: "The threat appears to be ongoing and the child is continually being sexually abused. It appears the child involved was sexually abused as early as last night." Comcast responded that the subscriber to the IP address was assigned to "Shelly Trader, 1189 SW Edinburgh Dr., Port St. Lucie, 34953..." (DE 1).

Agent Brant then appears to have enlisted the assistance of HSI agents in the Southern District of Florida. HSI Special Agent Brian Ray conducted a property records search for the 1189 Edinburgh Drive residence and learned that it was purchased by Leon Bonano and Shelly Trader-Bonano on June 16, 2016. He also conducted a drivers license records (DAVID) check of "Scott Trader." Scott Trader's residence address is listed in those records as 4286 Carl Street, Port St. Lucie, Florida. His mailing address was listed as 1189 S.W. Edinburgh Drive, Port St. Lucie, Florida. (PSR at 8-9).

Agent Ray also ran a criminal records check on Scott Trader. It showed that Mr. Trader had been charged with Promoting a Sexual Performance by a Child, Lewd Behavior, and Possession of Child Pornography in 2012. All of those charges were dismissed and Mr. Trader pled no contest to a single count of Child Neglect. Mr. Trader was not "convicted;" adjudication was withheld. In December of 2016, Mr. Trader was charged with Lewd Behavior. He has pled not guilty and was on bond at the time of his arrest in this case. He is presumed innocent. (PSR at 9).

Finally, Agent Ray conducted a brief surveillance of 1189 S.W. Edinburgh Drive and witnessed an adult woman and a female child, approximately two years of age, enter the residence. He never saw Mr. Trader during the surveillance. (DE 1).

HSI agents then applied for a search warrant for 1189 Edinburgh Drive. HSI Special Agent Lori Cercy submitted a sworn affidavit in which she related the investigation of Agents Brant and Ray. On May 31, 2017, The Honorable William Matthewman, United States Magistrate Judge, signed a search warrant for the residence. (DE 1).

On June 1, 2017, the search warrant was executed. In a bedroom allegedly shared by Mr. Trader and his wife, agents located two smart phones, nine SD cards, and a portable hard drive. A forensic examination of these items revealed evidence of child pornography. Some of the photos/videos allegedly depicted Mr. Trader involved in sexual behavior with minors. These items are the subject of the indictment in this case. (DE 1).

Standards of Review

This Court reviews a district court's denial of a motion to suppress evidence for clear error as to factual findings and *de novo* as to application of the law. *United States v. Watkins*, 760 F.3d 1271, 1282 (11th Cir. 2014).

Whether a search warrant affidavit states sufficient facts to establish probable cause is a question of law and is reviewed *de novo*. *United States v. Robinson*, 62 F.3d 1325, 1331 (11th Cir. 1995); *United States v. Miller*, 24 F.3d 1357, 1360 (11th Cir. 1994).

Whether a sentence is substantively unreasonable is reviewed under an abuse of discretion standard. *United States v. Irey*, 612 F.3d 1160, 1188 (11th Cir. 2010). "A district court abuses its discretion when it (1) fails to afford consideration to relevant factors that were due significant weight, (2) gives significant weight to an improper or irrelevant factor, or (3) commits a clear error of judgment in considering the proper factors. *Id.*, at 1189.

SUMMARY OF THE ARGUMENT

Law enforcement's procurement of location information, IP addresses, and email addresses, without a warrant, was an unlawful invasion in Mr. Trader's reasonable expectation of privacy in that information. In *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206 (2018), the Supreme Court announced that, even though compiled and maintained by a third party, location tracking data is protected by the Fourth Amendment and can only be obtained from those third parties by way of a warrant. The information obtained in this case included 30 days worth of location tracking and more. It also included IP addresses and the email address of the defendant. Law enforcement was required to obtain a warrant.

Despite this Court's recent opinion in *United States v. Joyner*, ____ F.3d ____, 2018 WL 385443 (11th Cir. August 14, 2018) permitting such pre-*Carpenter* searches without a warrant due to good faith, the government cannot now raise that defense because it did not preserve the argument below.

Next, the search warrant affidavit relied upon in this case failed to state sufficient probable cause to support the search. Specifically, the affidavit failed to establish a connection between the cellular telephone application used in the offense and the residence to be searched. Instead, the affidavit merely established a connection between a second cellular telephone application and the home to be searched based simply on a hunch that Mr. Trader was the user of both applications. No reasonable law enforcement officer would believe that, given those facts, the affidavit established probable cause.

Finally, Mr. Trader's sentence of life imprisonment is substantively unreasonable. Several of the enhancements applied under U.S.S.G. § 2G2.1 apply in almost every case. Those enhancements result in a sentence that is excessive, arbitrary, and not individualized. The sentencing court gave to much weight to those arbitrary guidelines and too little to other significant factors, such as Mr. Trader's mental health and acceptance of responsibility.

ARGUMENT AND CITATIONS OF AUTHORITY

<u>Issue I</u>

Whether the government's procurement of the defendant's "Kik" subscriber records, including location information, without warrant a was violation of Trader's Mr. reasonable privacy expectation under the Fourth Amendment.

The Fourth Amendment protects individuals from unreasonable searches and seizures. U.S. Const. Amend IV; Katz v. United States, 389 U.S. 347, 353, 88 S.Ct. 507, 512 (1967). Under the Fourth Amendment, a search occurs when the government intrudes into an area in which a person has a reasonable expectation of privacy. Kyllo v. United States, 533 U.S. 27, 33, 121 S.Ct. 2038, 2042 (2001). In the instant case, the government unreasonably invaded Mr. Trader's privacy by requesting records of his location and other Internet account information from Kik and Comcast under 18 U.S.C. § 2702(b) and (c). That evidence should have been suppressed, as well as any and all evidence emanating from that intrusion.

The United States Supreme Court has now made clear that the government may not require the production of third party records of an individual's movements over an extended time without a warrant based

upon probable cause. Carpenter v. United States, ___ U.S. ___, 138 S.Ct. 2206 (2018). In Carpenter, the government obtained two court ordered subpoenas for cell phone records of the defendant and several other individuals over a four month period. One of the subpoenas was for 127 days of records; the other was for only seven days of monitoring.² The defendant challenged the orders on the basis that they essentially monitored his personal movement during the periods in question. The government responded that the records were accessible under the "third party doctrine." Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577 (1979) (Voluntary release of records to third party relinquishes privacy interest), United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619 (1976) (same). The Carpenter trial court denied the motion to suppress and the Sixth Circuit affirmed the denial. United States v. Carpenter, 819 F. 3d 880 (6th Cir. 2017).

Granting the defendant's petition for a writ of certiorari, the Supreme Court reversed and refused to extend *Smith* and *Miller* to an individual's sensitive information regarding "physical movements." The Court found that cell phone data tracking was a "new phenomenon" in

² In response to the request for seven days of records, the provider only produced only two days of records. *Carpenter*, 138 S.Ct. at 2217, n. 3.

the government's ability to track people's past movements. Cell phone location data was captured regardless of the individual's knowledge or consent. There was no ability of the individual to disconnect from the The Court concluded that cell phone tracking records fall within the "modern day equivalents of an individual's own 'papers or effects' and should therefore receive the full protection of the Fourth Amendment. Carpenter, 138 S.Ct. at 2222. Finally, the Court rejected any quantitative threshold for the warrant requirement to apply. "[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." Id. at 2217, n. 3.

The Carpenter opinion also abrogated this Court's en banc opinion in United States v. Davis, 785 F.3d 498 (11th Cir. 2015), which, like the Sixth Circuit in Carpenter, had held that the government's acquisition of historical cell site records was not a search requiring a warrant because the defendant had knowingly permitted a third party to keep

those records. In the instant case, the government relied heavily on *Davis*, as did the district court. (DE 14:5); (DE 15:4–6).

The material in question in this case falls within the purview of *Carpenter*. The government requested and received 30 days worth of continuous monitoring of KiK, the cell phone application, and "subscriber identification information" from Comcast, the Internet provider. Each KiK entry reveals the exact time, the Internet Protocol Address ("IP Address"), and whether the user is accessing the Internet at the physical location of the Internet modem or whether the access was through a cellular device. The response also included the account user's Email address and the brand and model of the user's cell phone.

Through this information, law enforcement was able to monitor Mr. Trader's location on a regular basis throughout the 30 day period. In fact, HSI Special Agent Brian Ray relied on this location information in his search warrant affidavit to establish that Mr. Trader resided at the searched residence.

The type of information released in the instant case is arguably even more invasive and deserving of privacy protection than the CSLI obtained in *Carpenter*. First, the KiK response was primarily

information obtained from within the defendant's home. It is "a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable...'[A] greater burden is placed... on officials who enter a home or dwelling without consent. Freedom from intrusion into the home or dwelling is the archetype of the privacy protection secured by the Fourth Amendment." Payton v. New York, 445 U.S. 573, 586, 100 S.Ct. 1371, 1380 (1980) (quoting Dorman v. United States, 140 U.S.App.D.C. 313, 435 (1970)). By monitoring when Mr. Trader signed onto KiK through the modem in his home, law enforcement was conducting its search within the confines of his home without a warrant. Such a search is more intrusive than CSLI gathered from public locations.

Location monitoring is not the only privacy concern here. Law enforcement also requested, and KiK released the subscriber's "IP addresses." An IP address is the exact Internet electronic address of a particular Internet subscriber account. In addition to indicating the specific location of the user at the time of use, a significant portion of the user's Internet history could be recovered. A sophisticated and unscrupulous snooper can uncover intimate details about the user's

Internet activities. See, What Is An IP Address And What Can It Reveal About You, Cale Weissman, Business Insider, 2015, http://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5. Additionally, it is important to note that an IP address is not provided by the subscriber to an application provider such as "KiK." Instead, the IP address is assigned by the subscriber's Internet provider, without input or control of the subscriber.

Law enforcement also requested, and KiK released, the email address of the subscriber. As anyone in modern society knows, one's email address is often the first part of the secured entry process for Everything from bank account and credit card Internet accounts. access to on-line entertaining and dating services is now accessed through the use of one's email address. Revealing an email address can literally reveal the entirety of an individual's private life. concerns abound. See e.g., Five Reasons You Shouldn't Give Out Your EmailAddress, Adam Levin, ABC News. http://abcnews.go.com/Business/reasons-give-email-candy/story?id =*31373966*.

This Court has found that email addresses are "personal information" worthy of protection. See, e.g., United States v. Hastie, 854 F.3d 1298 (11th Cir. 2017) (email address is protected "personal information" under the Drivers Privacy Protection Act, 18 U.S.C. § 2721 et seq.) Other federal courts have recognized a right of privacy in one's email address as well. Government Accountability Project v. U.S. Department of State, 699 F.Supp. 2d 97 (D.C. 2010) (individual's right of privacy in email address precluded release under FOIA). Many states have also codified a right to privacy in one's personal email address. See, e.g., O.C.G.A. § 50–18–72(20)(A); Cal. Gov't Code § 6254.4; 5 Ill. Comp. Stat. 140/7(1)(c); Tex. Gov't Code § 552.102(a). These recognitions of the changing nature of modern communication support the conclusion that the protections announced in Carpenter should, and do, apply to the information requested and acquired by law enforcement in this case.

As noted, the release of an email address and IP address allow unscrupulous law enforcement or other third parties to examine the content and patterns of a subscriber's Internet use. Those pieces of private information were also sensitive information in which Mr. Trader had a reasonable and legitimate privacy interest. "The judiciary must not allow the ubiquity of technology---which threatens to cause greater and greater intrusions into our private lives---to erode our constitutional protections." *Davis*, 785 F.3d at 533 (J. Martin, dissenting).

Finally, the defendant acknowledges this Court's recent opinion in United States v. Joyner, ___ F.3d ___, 2018 WL 385443 (11th Cir. August 14, 2018), sustaining a search of CSLI, conducted prior to Carpenter and in good faith reliance on pre-Carpenter law. However, Joyner is not applicable in this case because the government failed to raise good faith in the district court and cannot raise it now for the first United States v. Carter, 110 F.3d 759 (11th Cir. 1997) time. (government waived defense by not raising it in the district court); United States v. Hansen, 956 F.2d 245 (11th Cir. 1992) (same). In Joyner, this Court specifically noted that the government had asserted a good faith defense "through out this case..." Joyner, at 4. In the instant case the government made no reliance upon good faith.³ cannot now raise that defense on appeal.

³ In contrast, in the trial court, the government expressly raised the defense of good faith to Mr. Trader's insufficiency of the warrant

Issue II

Whether the affidavit in support of the warrant to search Mr. Trader's home failed to show probable cause on its face.

Despite the fact that agents obtained a warrant to search the Trader residence, the warrant affidavit failed to state probable cause to believe that evidence of a crime committed by "Say Hi" user "Scott" would be found at the Trader house. The agents' substitution of information regarding "KiK" user "Daddyhasafunnyface" and his/her connection to the residence was insufficient to establish probable cause that evidence of the "Say Hi" crime would be found at the same house. There was no evidence that the IP address used by the "KiK' subscriber had been used any crimes whatsoever. And the idea that the IP address associated with the "KiK" account would be the same as that associated with the suspect "Say Hi" account was nothing more than a hunch on the part of agents.

Moreover, the agents could make little or no connection between Scott Trader and the residence to be searched---his mother's residence.

The mere listing of Mrs. Trader's residence as a mailing address for

application. See Government's Response To Defendant's Motion To Suppress, (DE 14:14–15).

Scott Trader with the Department of Motor Vehicles was insufficient for probable cause. This too was simply a hunch.

"It is critical to a showing of probable cause that the affidavit state facts sufficient to justify a conclusion that evidence or contraband will probably be found at the premises to be searched." United States v. Martin, 297 F.3d 1308 (11th Cir. 2002) (internal citations omitted) (emphasis added). Thus, the affidavit must contain "sufficient information to conclude that a fair probability existed that seizable evidence would be found in the place sought to be searched." Id. Specifically, the affidavit must establish a connection between the defendant and the residence to be searched and a link between the residence and any criminal activity. Id.

In the instant case, there was no connection shown between the residence to be searched and the alleged criminal activity on "Say Hi." The suspect user of "Say Hi," even if he/she was also the "Kik" user, could have used a million other IP addresses. Combined with the fact that the agents could establish little or no contact between the defendant and the residence to be searched, it is clear that probable cause did not exist.

In *United States v. Contreras-Rodriguez*, 291 Fed. Appx. 989 (11th Cir. 2008), this Court found probable cause lacking in a similar situation. There, agents applied for a search warrant based upon evidence that the property owners were housing and employing illegal aliens. The affidavit also requested leave to search other residences on the suspects' property, but failed to state probable cause connecting those other residences to the illegal activity. The court found the resulting warrant deficient, but denied exclusion based on *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 3420 (1984).

Had the agents in this case obtained the IP address from the "Say Hi" user and connected it to the Trader residence, probable cause may have existed. Instead, they just relied on a hunch that the IP address would be the same. That hunch was not probable cause. The effect of issuing a warrant based on the HSI agents' hypothesis was to sanction an exploratory search of the Trader residence based on a hunch, which is impermissible. See Andresen v. Maryland, 427 U.S. 463, 480, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976) (Fourth Amendment is designed specifically to prohibit the use of general warrants whereby the

authorities engage in "a general, exploratory rummaging in a person's belongings.").

Leon does not save the search in this case. The exclusionary rule does not bar the use of evidence seized by police officers acting in good faith reliance on a search warrant issued by a neutral and detached magistrate, even though it is later found to be deficient. However, the "good faith" exception to the exclusionary rule does not apply when: 1) the judge was intentionally misled by police in the search warrant affidavit; 2) the judge wholly abandoned her detached and neutral role; 3) the warrant was based upon an affidavit so lacking in probable cause as to render official belief in its existence entirely unreasonable; and 4) the warrant was so facially deficient by failing to particularize the place to be searched or things to be seized that reasonable officers could not presume it to be valid. United States v. Leon, 468 U.S. 897, 104 S.Ct. 3405 (1984).

In this case, as noted, the warrant affidavit was so lacking in probable cause that it was unreasonable for the officers to assume that it was valid. A reasonably well-trained officer would have known that the affidavit lacked probable cause.

"Our reading of *Leon* persuades us that the proper test is whether the *officer* acted in objective good faith under all the circumstances. The focus in *Leon* is on the officer. '[T]he officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable...." *United States v. Taxacher*, 902 F.2d 867, 871 (11th Cir. 1990) (quoting *Leon*, 486 U.S. at 918-19). "The good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id*.

The instant affidavit stated no connection between the residence or the IP address searched and any criminal activity whatsoever. A well-trained HSI special agent knows that a search warrant affidavit must state probable cause to believe that evidence of a specific crime will be found at a specific place to be searched. In this case, the agent was required to show that evidence of the "Say Hi" crime would probably be found at Mrs. Trader's residence. It was, and is, obvious that supplying the Court with the IP address for a separate Internet

application not connected with the suspect offense does not constitute probable cause. The agents did, or should have, known better.

Issue III

Whether Mr. Trader's sentence of life imprisonment was substantively unreasonable.

district court abused its discretion by imposing The unreasonable sentence and improperly weighing the 18 U.S.C. § 3553(a) factors. "A district court abuses its discretion when it (1) fails to afford consideration to relevant factors that were due significant weight, (2) gives significant weight to an improper or irrelevant factor, or (3) commits a clear error of judgment in considering the proper factors." *United States v. Irev.* 612 F.3d 1160, 1189 (11th Cir. 2010). In this case, the sentencing court gave too much weight to the outdated arbitrary sentencing guideline range and too little to Mr. Trader's personal history and characteristics and the goal of imposing an individualized Moreover, the outdated sentencing guidelines for child sentence. pornography cases resulted in an arbitrary and unfair sentencing guideline range which the lower court assumed was reasonable.

Mr. Trader was sentenced to life imprisonment, to be followed by lifetime supervised release. The sentence was within the sentencing

guideline range. The district court briefly mentioned Mr. Trader's history and personal characteristics in its summary of the evidence, but it did not give sufficient weight to those factors, or any mitigation at all, in arriving at a sentence. In doing so, the sentencing court, failed "to afford consideration to relevant factors that were due significant weight." *Irey*, 612 F.3d at 1189.

Federal sentencing guidelines are advisory and not binding on the sentencing court. United States v. Booker, 543 U.S. 220, 245, 125 S. Ct. 738, 756 (2005). Although the guidelines are "the starting point and the initial benchmark" for determining a sentence, the court "may not presume that the Guidelines range is reasonable." Gall v. United States, 552 U.S. 38, 49-50, 128 S.Ct. 586, 596-97 (2007); see also Irey, 612 F.3d at 1185 (stating that the abuse of discretion standard applies "whether the sentence is within or without the guidelines range"). Each sentence must be based on "an individualized assessment based on the facts presented." Gall, 552 U.S. at 50, 128 S. Ct. at 596. While district courts should "give respectful consideration to the Guidelines," they are permitted "to tailor the sentence in light of other statutory concerns as well." Kimbrough v. United States, 552 U.S. 85, 101, 128 S. Ct. 558, 570

(2007) (quoting at *Booker*, 543 U.S. 245-46). "[T]he Guidelines are not the only consideration . . . [and] the district judge should consider all of the § 3553(a) factors" to determine an appropriate sentence. *Gall*, 552 U.S. at 49-50, 125 S.Ct. at 596.

The § 3553(a) factors that sentencing courts must consider are:

- (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
- (2) the need for the sentence imposed--
- (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
- (B) to afford adequate deterrence to criminal conduct;
- (C) to protect the public from further crimes of the defendant; and
- (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
- (3) the kinds of sentences available;
- (4) the applicable guideline sentencing range;
- (5) pertinent policy statements issued by the Sentencing Commission;
- (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
- (7) the need to provide restitution to any victims of the offense.

18 U.S.C. § 3553(a).

The district court's sentence of life imprisonment was unreasonable and constitutes an abuse of its sentencing discretion

because the court presumed the guidelines to be reasonable. The district court based its sentence on the advisory guideline range, without evaluating whether the guidelines served their stated purpose or the factors enumerated in § 3553(a). This is evident when looking to the charged conduct and Mr. Trader's history and characteristics. He was convicted of a typical offense and had numerous mitigating of these personal characteristics. In light legal and factual considerations, a life imprisonment sentence was simply unreasonable.

The U.S.S.G. § 2G2.1 child pornography sentencing guidelines fail to serve the purposes of a criminal sentence as defined by the 18 U.S.C. § 3553(a) factors.

Congress enacted federal sentencing guidelines with three primary objectives: honesty, meaning that the sentence given at sentencing reflected the time to be served; uniformity, meaning that similar crimes by similar offenders received similar sentences; and proportionality, meaning that sentences should vary appropriately based on the offender's level of culpability. U.S. Sentencing Guidelines Manual, Ch. 1, Pt. A, introductory cmt. (2015).

The Sentencing Commission, along with an ever increasing number of federal courts, has concluded that the § 2G2.2 guidelines for child pornography offenses are inadequate to serve the goals of uniformity and proportionality. U.S. SENTENCING COMMISSION, REPORT TO CONGRESS: FEDERAL CHILD PORNOGRAPHY OFFENSES xii-xiii (2012) (finding that many stakeholders in the criminal justice system have concluded that current guidelines "fail[] to adequately differentiate among offenders based on their culpability," leading to "growing sentencing disparities among similarly situated offenders.") (Commission Report); see also 80 Fed. Reg. 36594 (June 25, 2015) (stating that one of the Sentencing Commission's top policy priorities for 2015-16 is enacting the reforms to child pornography sentencing explored in the 2012 commission report).

The Commission Report noted how current child pornography guidelines fail to promote proportionality. Current guidelines provide for enhancements based on factors existing in the vast majority of cases, i.e., for conduct involving: a) sadomasochistic content, b) prepubescent victims, c) use of a computer, and d) for possessing a large number of images. Commission Report at 209 (stating that such enhancements

apply in over 90 percent of cases in which an offender is convicted of a non-production offense); see also United States v. Grober, 624 F.3d 592, 608 (3d Cir. 2010); United States v. Diaz, 720 F. Supp. 2d 1039, 1042 (E.D. Wis. 2010). The report found that such enhancements often fail to distinguish between offenders based on their level of culpability. Commission Report xvii; See also, e.g., United States v. Dorvee, 616 F.3d 174, 187 (2d Cir. 2010) (explaining that "[t]he irrationality in § 2G2.2 is easily illustrated [by the fact that] [h]ad [the defendant] actually engaged in sexual conduct with a minor, his applicable Guidelines range could have been considerably lower"); United States v. Stone, 575 F.3d 83, 97 (1st Cir. 2009) (opining that § 2G2.2 is "in our judgment harsher than necessary" for many offenders); United States v. Beiermann, 599 F. Supp. 2d 1087, 1105 (N.D. Iowa 2009) ("This guideline . . . blurs logical differences between least and worst offenders, contrary to the goal of producing a sentence no greater than necessary to provide just punishment.").

The failure of the guidelines to calibrate sentences based on the individual relative culpability has led a growing consensus of courts to give below-guideline sentences in child pornography cases. Commission

Report xii-xiii (stating that in 2010, 78.8 percent of defendants received below-guideline sentences in such cases, including 44.3 percent of defendants receiving below-guideline sentences not endorsed by the government). Because of this, most offenders are subject to long guideline ranges and arbitrary decisions about whether those ranges should be adopted. Commission Report xii-xiii (2012) (concluding that "no offender or offense characteristics . . . appeared to account for [below - guideline sentencing] practices in most cases," but rather the differences were primarily attributable to "geographical differences").

U.S.S.G. § 2G2.1, under which Mr. Trader's sentencing guidelines were scored, suffers from many of the same flaws. Involving the commission of a sexual act, distribution, and sadistic or masochistic conduct are all enhancements that occur in the vast majority of section 2G2.1 cases. The application of these enhancements results in arbitrary and excessive sentences in this and other cases.

Additionally, numerous offenses of equal or greater seriousness have lower offense levels. First degree murder is such an offense. Under U.S.S.G. § 2A1.1, the offense level for first degree murder, *before acceptance*, is 43. With a three point reduction for acceptance it is level

40. Given Mr. Trader's criminal history category of III, he would have a guideline range of 360 months to life if he had been convicted of first degree murder. Second degree murder (§ 4A1.2) would carry a total offense level of 35 after acceptance, with a range of 210–262 months. Attempted murder for pecuniary gain, causing permanent bodily injury, would result in an offense level of 38 after acceptance and a guideline range of 292–365 months.

Likewise, kidnapping (§ 4A4.1) with permanent bodily injury, use of a firearm, and sexual exploitation of the victim would result in an offense level of 41 after acceptance and a guideline range of 360–life. Hijacking (§ 4A5.1) resulting in death has an offense level of 40 after acceptance and a guideline range of 360–life.

Perhaps most informative in this regard is the guideline for "Criminal Sexual Abuse" (§ 2A3.1). A defendant convicted of criminal sexual abuse of a prepubescent minor in his care and custody, would have an offense level of 37 after acceptance and a guideline range of 262–327 months. Even if the "pattern" enhancement from U.S.S.G. § 4B1.5(b) were applied, the offense level would be 42 after acceptance.

All of these offenses are equally serious, or more serious, than the production of child pornography or enticement of a minor offenses under the facts of this case. Consequently, Mr. Trader maintains the sentencing guideline range in this and other like cases is arbitrary and a sentence lower than "life" is appropriate.

These arbitrary and excessive sentencing guideline ranges have resulted in another effect that violates the intent of § 3553(a). That is a lack of uniformity in child pornography sentences. Because a significant number of courts no longer accept the enhancement structure of § 2G2.2 and regularly vary downward from the guideline range, the issue has created a distinct sentencing range disparity between those sentenced by courts who follow the enhancement structure and those who do not. Thus, the guidelines no longer serve the purpose of creating a "heartland" of typical child pornography cases that warrant guideline sentences. They do just the opposite. The disparity and lack of uniformity are directly contrary to Congress' intent in § 3553(a), the mandatory cornerstone of federal sentencing.

In light of this failure to achieve two of the three primary goals of the sentencing guidelines, the § 2G2.1 enhancement scheme violates

many of the § 3553(a) factors that sentencing courts are required to consider. When sentences are arbitrary, it lessens respect for the law means for providing just punishment. See 18 U.S.C. § asAs explored above, § 2G2.1 has failed to "avoid 3553(a)(2)(A). unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). Such disparities also erode the deterrent effect of escalating sentences for more serious offenses. 18 U.S.C. § 3553(a)(2)(B); Kennedy v. Louisiana, 554 U.S. 407, 445-46, 128 S. Ct. 2641, 2664 (2008) (explaining that imposing the same sentence for more and less culpable conduct may prevent deterrence of the more culpable conduct). Finally, and most clearly, the guidelines are out of step with the "pertinent policy statements issued by the Sentencing Commission." 18 U.S.C. § 3553(a)(5).

These distortions of § 3553(a) are clearly evident in Mr. Trader's case. He received 8 additional offense levels due to "run of the mill" enhancements in § 2G2.1, two for the commission of a sexual act or sexual contact, two for distribution, and four for sadomasochistic

content.⁴ Those enhancements, which are common and in no way unique to Mr. Trader, dramatically enhanced the guideline range from a base offense level of 32, to level 40. In no way can his sentencing range said to have been individualized to either his conduct or his characteristics.

Moreover, by providing such an arbitrary and artificially high sentencing range, the § 2G2.1 enhancements overwhelm the other equally important and mandatory considerations of § 3553(a). In particular in the instant case, the sentencing court gave excessive consideration to the arbitrary guideline range and insufficient weight to other considerations, such as Mr. Trader's age, family ties, lack of serious criminal history, contributions to the community, and cooperation with authorities.

The heartland of child pornography sentences has shifted. The Sentencing Commission has reported that the specific offense characteristics, once thought relevant to individualized culpability, are no longer significant considering the changed nature of the offense.

⁴ It should also be noted that Mr. Trader received a five offense level increase for a "pattern" of behavior, that being the alleged abuse of his daughter. Thus, this factor was also arguably overrepresented in the guideline computation. (PSR at 25).

Because courts, and even prosecutors, have recognized the overseverity and disproportionate nature of these sentences, the guideline range no longer reflects a typical child pornography offense. Assigning an offender, such as Mr. Trader, a guideline sentence does not serve to promote proportionality or uniformity in sentencing. And it does not provide the individualized sentence required by *Gall*.

The district court concluded that a within-guidelines sentence would be reasonable. However, the § 2G2.1 guidelines for child pornography do not warrant such deference because they do not promote the underlying required goals of § 3553(a). Thus, the district court abused its discretion by giving too much weight to the guideline recommendation and "fail[ing] to afford consideration to [other] relevant factors that were due significant weight." *Irey*, 612 F.3d at 1189 (quoting *United States v. Campa*, 459 F.3d at 1174).

CONCLUSION

For the foregoing reasons, this Court must reverse Mr. Trader's conviction and remand with instructions that he be permitted to withdraw his guilty plea, or in the alternative, that his sentence be vacated and the case remanded to the district court for resentencing.

MICHAEL CARUSO FEDERAL PUBLIC DEFENDER

s/Fletcher Peacock_

Fletcher Peacock
Assistant Federal Public Defender
109 North 2nd Street
Fort Pierce, Florida 34950
Telephone No. (772) 489-2123
Email: fletcher_peacock@fd.org

CERTIFICATE OF COMPLIANCE

I CERTIFY that this brief complies with the type-volume limitation and typeface requirements of Fed. R. App. P. 32(a)(7)(B), because it contains 7,048 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief also complies with the requirements of Fed. R. App. P. 32(a)(5) and (a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14 point, Century Schoolbook font.

s/Fletcher Peacock
Fletcher Peacock

CERTIFICATE OF SERVICE

I HEREBY certify that on this 10th day of September, 2018, I

electronically filed the foregoing document with the Clerk of the Court

using CM/ECF and sent seven copies to the Clerk of the Court via third

party commercial carrier for delivery within three days. I also certify

that the foregoing document is being served this day via CM/ECF on

Emily M. Smachetti, Chief, Appellate Division, United States

Attorney's Office, 99 N.E. 4th Street, Miami, Florida 33132.

<u>s/Fletcher Peacock</u>

Fletcher Peacock